INTIMIDADE DIGITAL E PERSECUÇÃO PENAL: Fundamentos legais e requisitos para quebra de sigilo em dispositivos móveis e plataformas digitais sob a ótica dos tribunais[1]

DIGITAL INTIMACY AND CRIMINAL PROSECUTION: legal foundations and requirements for breaching confidentiality on mobile devices and digital platforms from the perspective of the courts

GUIMARÃES, Michel da Silva[2]

ROCHA, Theotonio Ribeiro Junqueira[3]

FELIX, Danielle Rodrigues[4]

RESUMO

A presente pesquisa tem como objetivo compreender os principais debates e entendimentos jurisprudenciais acerca dos requisitos legais para a relativização da proteção da intimidade e à vida privada que se desenvolveu no mudo digital. Para tanto, realizou-se uma análise jurisprudencial em busca dos fundamentos que legitimam o acesso estatal a dados pessoais, especialmente aqueles armazenados em dispositivos móveis e acessíveis pelas plataformas digitais (armazenadas em nuvem). Assim, no presente trabalho, foram analisados os principais embates que envolvem a coleta de provas digitais, com foco nas seguintes questões: (i) qual a autoridade é legitimada para solicitar dados estáticos e telemáticos; (ii) a necessidade de autorização judicial para acesso aos dados de aparelhos apreendidos no momento de um flagrante policial; (iii) a não exigência de autorização especifica para extração de dados de aparelhos apreendidos no cumprimento de mandado de busca e apreensão; e (iv) os limites da requisição de dados às empresas prestadoras de serviços digitais (*Google*; *Apple*; *Facebook*, entre outras). Para responder a essas questões, o estudo realizou uma leitura crítica da jurisprudência nacional, aliada à doutrina, com o intuito de esclarecer, de forma qualitativa, os contornos legais que protegem a intimidade e a vida privada no ambiente digital frente à atuação Estatal no âmbito da persecução penal.

Palavras-chave: intimidade digital; vida privada; quebra de sigilo; persecução penal; prova digital.

ABSTRACT

This research aims to understand the main debates and jurisprudential understandings regarding the legal requirements for the relativization of the protection of privacy and private life that has developed in the digital world. To this end, a jurisprudential analysis

---

[1] Trabalho de Conclusão de Curso apresentado à Faculdade FacMais de Ituiutaba, como requisito parcial para a obtenção do título de Bacharel em Direito no segundo semestre de 2025.

[2] Acadêmico do 10º Período do curso de Direito pela Faculdade Mais de Ituiutaba - FacMais. E- mail: michel.guimaraes@aluno.facmais.edu.br

[3] Acadêmico do 10º Período do curso de Direito pela Faculdade Mais de Ituiutaba - FacMais. E- mail: theotonio.rocha@aluno.facmais.edu.br

[4] Professora-Orientadora - Especialista em Direito Processual Civil e Direito Civil. Docente da Faculdade Mais de Ituiutaba - FacMais. E- mail: danielle.felix@facmais.edu.br

was conducted to find the foundations that legitimize state access to personal data, especially data stored on mobile devices and accessible through digital platforms (stored in the cloud). Thus, this work analyzed the main debates involving the collection of digital evidence, focusing on the following questions: (i) which authority is legitimized to request static and telematic data; (ii) the need for judicial authorization to access data from devices seized during a police raid; (iii) the non-requirement of specific authorization for the extraction of data from devices seized during the execution of a search and seizure warrant; and (iv) the limits of data requests to digital service providers (Google, Apple, Facebook, among others). To answer these questions, the study conducted a critical reading of national jurisprudence, combined with legal doctrine, in order to qualitatively clarify the legal contours that protect privacy and private life in the digital environment in the face of State action within the scope of criminal prosecution.

Keywords: digital privacy; private life; breach of confidentiality; criminal prosecution; digital evidence.

1 INTRODUÇÃO

A tecnologia disponível em nossas mãos nos coloca à disposição uma série de recursos e aplicativos que, por meio da sua capacidade de armazenamento e seu potencial de comunicação, tornou-se um plano existencial que tende a ser uma realidade imaterial que, de fato, se transformou em uma extensão da intimidade do indivíduo, um abrigo da vida privada (Lopes Júnior, 2025, p. 499).

Aury Lopes Junior leciona que o conjunto de “informações, imagens, vídeos, áudios, trajetos, leituras, redes sociais etc.”, acessíveis por meio dos *Iphones* e *smartphones*, são “uma verdadeira extensão da personalidade do agente e, de certa forma, um asilo inviolável do indivíduo, um lar do ser, que exige proteção” (Lopes Junior, 2025, p. 500).

Em síntese, os aparelhos e aplicativos que nos conectam (via internet) neste ambiente virtual, diante do vasto conjunto de dados pessoais, tornaram-se em uma metrópole informacional da personalidade do indivíduo que, de fato, necessita de ampla proteção frente aos excessos que podem ser cometidos em nome da persecução penal. Isso porque, o Estado, ao violar um aparelho ou seus dados, corre o risco de ferir direitos fundamentais que derivam da dignidade da pessoa humana, tais como a intimidade[5], vida privada[6], imagem, sigilo da comunicação e dos dados telemáticos e estáticos, podendo, até mesmo, violar o direito da não autoincriminação.

A priori, devemos compreender que: “O combate ao crime não pode ocorrer com atropelo da ordem jurídica nacional, sob pena de vir a grassar regime totalitário, com prejuízo para toda a sociedade’’ (STF – 2. T., HC nº 74639-0/RJ – rel. Min. Marco Aurélio, Diário da Justiça, 31-10-1996).

De acordo com os relatórios de transparência da empresa *Google*, que disponibiliza dados sobre as solicitações de informações de usuários feitas pelas instituições governamentais, é possível notar que, somente no primeiro semestre de 2020, houve 103.816 solicitações de divulgação de informações sobre determinado usuário e 235.434 solicitações de informações de contas. Em 2024, esse número mais

[5] “Integram a intimidade, por exemplo, a convicção política, religiosa ou orientação sexual” (Morais, 2022).

[6] “a privacidade importa na relação com outra pessoa, sendo que aquela não pode sofrer intervenção de terceiros, salvo nas hipóteses autorizadas pela lei” (Morais, 2022).

do que dobrou, passando para 236.520 solicitações de divulgação de informações sobre determinado usuário e 510.794 solicitações de informações de contas[7].

De igual modo, por meio dos relatórios de transparência divulgados pela empresa *Apple*, as instituições brasileiras requisitaram, por meio de solicitação de dispositivo (8.776), identificador financeiro (12), conta (3.664), push token (0) e emergência (67), um total de 12.519 solicitações de dados dos usuários no primeiro semestre de 2024. Uma diferença gritante se comparado com o primeiro semestre de 2020, em que a empresa registrou 2.615 solicitações[8].

Nessa nova perspectiva processual, os elementos probatórios passaram de pequenas pastas cheias de papéis para um universo composto vários *bytes*, *megabytes* e, até mesmo, *terabytes* de dados/informações armazenados em "nuvem".

Assim, com a nova estrutura tecnológica social, houve uma mudança significativa no processo penal. O procedimento de uma investigação criminal ganhou novos rumos ao migrar para um plano probatório imaterial da vida privada, construído pelo próprio sujeito.

De fato, há uma extensão da intimidade que se digitaliza em um mundo cibernético e nos inquieta saber quais os limites do Estado para relativizar sua inviolabilidade e produzir, antecipadamente ou no curso do processo, a fonte probatória que impulsionará o processo e servirá de base para uma decisão judicial.

Em síntese, busca-se compreender a atuação estatal e os requisitos que devem ser preenchidos quanto à medida cautelar que decreta a relativização da proteção constitucional da intimidade que se explora em meio aos dados disponíveis em armazenamento estático (do próprio aparelho) e pelas empresas com capacidade de operar dados telemáticos que, como veremos, ocorre até por meio congelamento/armazenamento compulsório de dados.

Visto às incertezas que orbitam as garantias constitucionais neste cenário de constante evolução tecnológica, em que inúmeras são as hipóteses em que o Estado, por meio de seus agentes, em busca de soluções para as demandas atuais, utilizam-se da extensão digitalizada da intimidade que se extraí dos aparelhos (apreendidos) e do uso de aplicativos com capacidade de armazenamento (backup/nuvem) de dados pessoais, para fins de persecução penal, neste estudo, busca-se resposta(s) para o seguinte questionamento: **Quais os entendimentos jurisprudenciais sobre os parâmetros de proteção da intimidade digital e os requisitos da ordem judicial que permite a violação de dados, sob a ótica dos tribunais?**

Para responder essa questão, foi proposto o seguinte objetivo geral: **Compreender os parâmetros de proteção da intimidade e os limites e requisitos para a quebra de sigilo de dados armazenados nos aparelhos e pelos provedores de serviços na internet (ex: *Google*, *Apple*, *Meta*, etc.).** Quanto aos objetivos específicos, propôs-se, nesse estudo: i) percorrer a legislação vigente aplicada em casos concretos de violação da intimidade construída no mundo digital para fins de promoção da persecução penal; ii) analisar jurisprudências acerca de casos que envolvem a violação da intimidade; e iii) refletir sobre os efeitos dessa mudança que houve no cenário da persecução penal e sua adequação às garantias constitucionais.

---

[7] Solicitações globais de informações de usuários. **Google**, 2025. Disponível em: https://transparencyreport.google.com/user-data/overview?hl=pt_BR&user_data_produced=authority:BR;series:compliance&lu=user_data_produced. Acesso em: 20 ago. 2025.

[8] Transparency Report. **Apple**, 2025. Disponível em: https://www.apple.com/legal/transparency/. Acesso em: 20 ago. 2025.

Esse novo paradigma da persecução penal, notadamente, pauta-se pela relativização de direitos fundamentais e, de fato, propõe ao mundo acadêmico e jurídico a necessidade de compreender a operacionalidade do interesse público para que, a atuação estatal e o processo penal, sejam guiados pelos princípios constitucionais que sustentam o Estado Democrático de Direito.

2 PARÂMETROS LEGAIS DE PROTEÇÃO DA INTIMIDADE QUE SE EXTRAI DOS DADOS TELEMÁTICOS

Hodiernamente, devido à grande metrópole de dados e metadados armazenados, a dimensão da intimidade que se revela em tais aparelhos e aplicativos, pela sua capacidade de desnudar a intimidade e a vida privada de um indivíduo, tornaram-se, para o processo penal, fontes úteis para construção da verdade real (Lopes Junior, 2025).

Entretanto, existem limites e garantias constitucionais e, de fato, a intimidade do indivíduo deve ser compreendida como “um espaço íntimo intransponível por intromissões ilícitas externas” (Moraes, 2025, p. 73), seja pelo Estado ou por terceiros.

A proteção à intimidade estabeleceu contornos sólidos no cenário jurídico internacional no pós-Segunda Guerra Mundial, período que sucedeu um momento histórico marcado pelos excessos causados pela utilização do Estado Alemão para manutenção dos ideais nazistas.

Após cessar os abusos cometidos pelo regime totalitário marcado por guerras, a proteção da intimidade, como garantia fundamental aos cidadãos, veio expressa no artigo 12 da Declaração Universal dos Direitos Humanos de 1948, com a seguinte redação: “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei” (ONU, 1948).

No Brasil, após findar a Ditadura Militar, regime marcado pela barbárie, a proteção da intimidade e da vida privada se consolidou com a Constituição Federal de 1988. O inciso X, do artigo 5°, da Carta Magna brasileira garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, sendo certo que deve ser assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Lado outro, o inciso XII estabelece, como direito fundamental, a inviolabilidade do “sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (Brasil, 1988).

O ordenamento jurídico pátrio, com o decreto n° 678, de 6 de novembro de 1992, ratificou a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. No artigo 11 do respectivo diploma supralegal veio expresso o dever de ser promovido, pelo Estado, a proteção da honra e da dignidade das pessoas, garantindo que ninguém seja objeto de “ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação” (Brasil, 1992).

Aqui, um contraponto, por mais que a intimidade tenha adquirido proteção nacional e internacional, conforme ensina o Ministro Alexandre de Moraes, para não descredibilizar a atuação estatal, os direitos adquiridos constitucionalmente “não podem ser utilizados como um verdadeiro escudo protetivo da prática de atividades

ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos" (Moraes, 2025, p. 38).

Com a entrada em vigor das leis 12.965/14 conhecida por Marco Civil da Internet e a lei 13.709/18, Lei Geral de Proteção de Dados (LGPD), nosso ordenamento jurídico iniciou de maneira efetiva a regulamentação e proteção dos bens jurídicos que se materializam no mundo digital.

Por meio da Lei 12.965/14 restaram estabelecidos princípios, garantias, direitos e deveres para o uso e gestão da internet no território brasileiro e determinadas diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. O diploma trouxe, no inciso II, do art. 3º, a garantia de proteção da privacidade daqueles que usam a internet no Brasil, sendo um princípio basilar dos tempos atuais (Brasil, 2014).

Além de estabelecer princípios e conceitos importantes, a referida lei estabelece direitos e garantias aos usuários da internet. Dentre eles, estão a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei e a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (Brasil, 2014, art. 7°, I, II e III).

Por sua vez, a Lei 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD), surge com o objetivo de reforçar os direitos fundamentais da liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural. Para cumprir essa necessidade, o poder legislativo determinou que a pessoa natural ou jurídica, que exerça alguma atividade que resulte em tratamento de dados, seja ofertando ou fornecendo bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional, devem agir com respeito à privacidade (Brasil, 2018, art. 2º, I) e garantir a inviolabilidade da intimidade, da honra e da imagem (Brasil, 2018, art. 2º, IV), com respeito aos direitos humanos, promovendo o livre desenvolvimento da personalidade, da dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018, art. 2º, VII).

Entretanto, o legislador restringiu, no art. 4º, sua aplicação ao tratamento de dados pessoais no caso de atividades de investigação e repressão de infrações penais (Brasil, 2018, art. 4º). Ora, por mais que haja previsão de não se aplicar em atividades de investigação e repressão de infrações penais, existem limites que devem conduzir a persecução penal.

Assim, visto que as garantias constitucionais não possuem caráter absoluto e podem ser relativizadas, o legislador necessitou adaptar o ordenamento jurídico aos atuais contornos da persecução penal e aos julgadores, cabe sua aplicação nos casos concretos. Conforme será analisado a seguir.

3 ANÁLISE JURISPRUDENCIAL DA APLICABILIDADE DOS PARÂMETROS DE PROTEÇÃO DA INTIMIDADE QUE SE EXTRAI DE APARELHOS CELULARES EM POSSE DA AUTORIDADE POLICIAL.

Importante se faz a análise da competência para solicitar e realizar a quebra de sigilo do aparelho em posse do investigado e analisar os dados extraídos dos aparelhos apreendidos no flagrante ou cumprimento de mandado.

No tocante ao papel da polícia brasileira, observamos que, de acordo com a Constituição, no § 4º, do art. 144, cabe às polícias civis, dirigidas por delegados de polícia de carreira, ressalvada a competência da União, as funções de polícia judiciária

e a apuração de infrações penais, salvo as militares. Quanto aos policiais militares, o § 5º determina a realização do policiamento ostensivo e a preservação da ordem pública (Brasil, 1988).

Lado outro, a polícia federal é instituída por lei como um órgão permanente, que deve ser organizado e mantido pela União, destinando à realização de apuração de "infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei" (Brasil, 1988, art. 144, § 1º).

Além disso, cabe aos agentes públicos federais "prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência". Deve também "exercer as funções de polícia marítima, aeroportuária e de fronteiras" e "as funções de polícia judiciária da União" (Brasil, 1988, art.144, §1º, I, II, III e IV,). Vale ressaltar que não há óbice quanto à atuação da polícia civil na repressão do tráfico de drogas.

Quanto ao policiamento preventivo ou ostensivo que, de fato, é realizado pelas polícias militares dos estados e Distrito Federal, em regra, não gozam da atribuição para conduzir a investigação preliminar, pois, de fato, o inquérito policial está a cargo da polícia judiciária. A exceção para a regra, conforme ensina Aury Lopes Junior, ocorre quanto aos crimes previstos no Código Penal Militar. Porém, por mais que os papéis das polícias brasileiras sejam distintos (a polícia judiciária e a polícia preventiva), na prática, nem sempre isso ocorre (Lopes Junior, 2025, p. 111).

No Brasil, cabe à polícia judiciária realizar a investigação preliminar que antecede o processo, devendo ser desempenhada, pela autoridade policial competente, nos estados e distrito federal pela Polícia Civil e, no âmbito federal, pela Polícia Federal. Vale destacar os ensinamentos de Aury Lopes Junior (2025):

> A investigação preliminar situa-se na fase pré-processual, sendo o gênero do qual são espécies o inquérito policial, as comissões parlamentares de inquérito, sindicâncias etc. Constitui o conjunto de atividades desenvolvidas concatenadamente por órgãos do Estado, a partir de uma notícia-crime, com caráter prévio e de natureza preparatória com relação ao processo penal, e que pretende averiguar a autoria e as circunstâncias de um fato aparentemente delituoso, com o fim de justificar o processo ou o não processo (Lopes Junior, 2025, p.106).

Pontuamos que o presente trabalho tende a se limitar à análise da necessidade intervenção judicial para a adoção de medidas restritivas de direitos fundamentais na atuação policial. Logo, conforme explica o renomado jurista, o inquérito policial "é um modelo de investigação preliminar policial" em que "a polícia judiciária leva a cabo o inquérito policial com autonomia e controle" (Lopes Júnior, 2025, p. 111).

De acordo com o § 2.º do artigo 2.º da Lei n.º 12.830, de 2013, cabe "ao delegado de polícia requisitar dados que interessem ao esclarecimento do crime, porém não especifica quais poderão ser requisitados sem a intervenção do Poder Judiciário" (Morais, 2022).

A Lei n.º 13.344, de 2016, incluiu o artigo 13-A ao Código de Processo Penal, estabelecendo a possibilidade da autoridade policial ou o Ministério Público requisitar dados cadastrais qualificação pessoal, filiação e endereço mantidos operadoras de telefonia, instituições financeiras, provedores de *internet* e administradoras de cartão de crédito.

> Art. 13-A. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos (Brasil, 1940).

Ademais, o art. 13-B da Lei 2.848/40 preleciona que:

> Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso (Brasil,1940).

A jurisprudência tem adotado a tese de que não há "distinção entre as atividades da polícia judiciária e da polícia investigativa". Isso porque, conforme se extrai do julgado em análise, a Constituição da República não veda a realização de investigações pela polícia militar. Assim decidiu o des. Antônio Zoldan da Veiga, da 5ª Câmara Criminal do TJSC, e firmou o entendimento de que, em caso de inquérito realizado pela polícia militar, não há suposta usurpação de atribuição exclusiva da polícia civil[9].

Portanto, é possível ver que o judiciário está flexibilizando o princípio da legalidade ao permitir que uma polícia exerça a função da outra. Nucci, muito bem ensina que não podemos desgarrar à atuação policial das limitações constitucionais e admitir ampla discricionariedade para sua atuação em nome da segurança pública. (Nucci, 2025, p. 359)

À vista disso, além do possível despreparo técnico, caso uma polícia cumpra a função da outra, estará deixando de cumprir sua função precípua, aquilo que constitucionalmente se espera. Talvez seja por conta da usurpação de atribuições que, repetidamente, conforme será analisado adiante, presenciamos vários casos de violação da intimidade durante abordagens policiais. Legitimar tal conduta é fortalecer o arbítrio já praticado no policiamento ostensivo.

O Ministério Público é legalmente autorizado a requerer abertura como também acompanhar a atividade policial no curso do inquérito. A ressalva da doutrina se dá pela ausência:

> [...] de uma norma que satisfatoriamente defina o chamado controle externo da atividade policial – subordinação ou dependência funcional da polícia em relação ao MP –, não podemos afirmar que o Ministério Público pode assumir o mando do inquérito policial, mas sim participar ativamente, requerendo diligências e acompanhando a atividade policial (Lopes Junior, 2025, p. 112).

Destarte, assim como a figura do Delegado de Polícia pode requerer a quebra de sigilo, pode também o Promotor. Contudo, existem requisitos, e a autorização judicial que posterga a inviolabilidade da intimidade para colheita de provas, para que sejam processualmente válidos os dados obtidos, deve ocorrer em respeito às regras constitucionais e processuais.

---

[9] SANTA CATARINA. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus Criminal nº 5033494-87.2021.8.24.0000**. Relator: Des. Antônio Zoldan da Veiga. Julgado em: 15 jul. 2021.

Presume-se que, ao apreender alguém em flagrante delito, a polícia militar deverá conduzi-lo, junto os objetos apreendidos em sua posse, à presença da autoridade policial (Delegado), para que este coloque o conduzido à disposição do juiz e adote ou não algumas medidas cautelares (quebra de sigilo; prisão) que se observem necessárias ao andamento do inquérito. Porém, ocorre que, após realizar uma prisão em flagrante e/ou cumprimento de mandado de busca e apreensão, a polícia militar e/ou a autoridade policial, em algumas hipóteses, utilizam da intimidade que se extrai de um aparelho telefone sem prévia autorização judicial.

3.1 Violação de aparelhos apreendidos no momento do flagrante e em cumprimento de mandado de busca e apreensão

A priori, devemos compreender que, de acordo com o entendimento do Superior Tribunal de Justiça, a perícia em dados de celular apreendidos em situação de flagrante, por violar o direito à intimidade e à inviolabilidade de dados, não é possível ser realizada sem prévia autorização judicial. Esse entendimento tem sido adotado pelos tribunais, reiteradamente, garantindo a necessidade de autorização para obter acesso aos dados existentes em um aparelho celular. Portanto, a autoridade policial deve obter prévia autorização judicial para ter acesso às mensagens contidas em aparelho celular apreendido[10]. Seguindo esse entendimento, o Desembargador Federal, Paulo Gustavo Guedes Fontes, da 5° turma do TRF3, entendeu que:

> É ilícita a prova obtida diretamente dos dados constantes de aparelho celular, decorrentes de mensagens de textos SMS, conversas por meio de programa ou aplicativos ("WhatsApp"), mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no momento do flagrante, sem prévia autorização judicial para análise dos dados armazenados no telefone móvel (...).[11]

Em decisão cirúrgica, o Min. Nefi Cordeiro, ao fixar a seguinte tese: “Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido por ocasião da prisão em flagrante, sem prévia autorização judicial”, reconheceu a nulidade das provas obtidas por meio do ingresso domiciliar sem mandado, bem como do acesso ao celular do paciente, sem autorização judicial, e determinou, visto a ilicitude, seu desentranhamento dos autos[12].

Conforme ensina Aury Lopes Júnior, no Brasil, “o legislador consagrou o caráter pré-cautelar da prisão em flagrante”. O autor, citando Banacloche Palao, explica que:

> o flagrante – ou la detención imputativa – não é uma medida cautelar pessoal, mas sim pré-cautelar, no sentido de que não se dirige a garantir o resultado final do processo, mas apenas destina-se a colocar o detido à disposição do juiz para que adote ou não uma verdadeira medida cautelar. Por isso, o autor

---

[10] BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo em Recurso Especial nº 2.697.584/MG**. Relatora: Min. Daniela Teixeira. Julgado em: 17 dez. 2024.

[11] BRASIL. Tribunal Regional Federal da 3ª Região (5. Turma). **Apelação Criminal nº 0003512-51.2013.4.03.6002**. Relator: Des. Fed. Paulo Gustavo Guedes Fontes. Julgado em: 18 set. 2020. Publicado em: 24 set. 2020.

[12] BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 617.232/SP**. Relator: Min. Nefi Cordeiro. Julgado em: 23 fev. 2021.

> afirma que é uma medida independente, frisando o caráter instrumental e ao mesmo tempo autônomo do flagrante (Lopes Júnior, 2025, p. 737).

Porém, por mais que exista um caráter pré-cautelar na prisão em flagrante, conforme assentado pela corte do STJ, "é ilícita a tomada de dados, bem como das conversas de Whatsapp, obtidas diretamente pela autoridade policial em aparelho celular apreendido no flagrante, sem prévia autorização judicial"[13]. Assim, ao realizar o flagrante, a autoridade policial, na posse de um aparelho apreendido, deverá obter autorização judicial para ter acesso ao conteúdo.

Frente à necessidade de análise da legalidade quebra de sigilo decretada após flagrante delito, o Desembargador Federal Ângelo Roberto Ilha da Silva, da 7ª turma do TRF4, fundamentou a legalidade da cautelar tendo em vista que não há de se cogitar a nulidade da decisão que defere a quebra do sigilo de aparelho celular apreendido durante o flagrante de um crime. Isso porque, de acordo com o relator, no caso em análise, a fundamentação da decisão teve respaldo na necessidade de "delimitar as circunstâncias do fato e apurar a eventual participação de terceiros na prática delitiva"[14].

No mesmo sentido, a Desembargadora do Tribunal de Justiça de Minas Gerais, Maria Luíza de Marilac, seguindo os parâmetros estabelecidos pelos tribunais superiores, em defesa das garantias individuais, reconheceu a ilicitude da abordagem realizada por policiais militares, em via pública, que culminou na "devassa do aparelho celular" e das buscas em domicílio realizadas posteriormente (provas derivadas) justificando que "se basearam exclusivamente no teor de mensagens indevidamente obtidas". A desembargadora sustenta que a intromissão do agente no aparelho "constitui situação não albergada pelo comando do art. 5º, inciso XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações"[15].

Em sentido oposto e flexibilizando os limites da atuação policial no tocante ao atendimento de ligação telefônica durante o contexto de flagrante delito, o Desembargador Rubens Rollo D'Oliveira entendeu que não é necessário autorização judicial prévia e fundamentou a licitude do ato alegando que, por não configurar interceptação telefônica, que está sujeita à Lei nº 9.296/1996, fica dispensando a obrigatoriedade de autorização judicial prévia. De acordo com o prolator da decisão, a "ação constitui procedimento policial legítimo, visando evitar a continuidade do crime e garantir a ordem pública"[16]. Tal decisão vai de encontro com o entendimento do STJ.

O Ministro Sebastião Reis Júnior, ao analisar o caso em que o policial atendeu ao telefone e obteve acesso à dados e mensagens por meio do aparelho, sem autorização, se passando pela pessoa abordada e realizando negociações de compra ou venda de drogas para provocar o flagrante, entendeu que:

> Não tendo a autoridade policial permissão, do titular da linha telefônica ou mesmo da Justiça, para ler mensagens nem para atender ao telefone móvel da pessoa sob investigação e travar conversa por meio do aparelho com

---

[13] BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 674.185/MG**. Relator: Min. Sebastião Reis Júnior. Julgado em: 17 ago. 2021.

[14] BRASIL. Tribunal Regional Federal da 4ª Região (7. Turma). **Habeas Corpus nº 5018214-96.2023.4.04.0000/RS**. Relator: Des. Fed. Angelo Roberto Ilha da Silva. Julgado em: 22 jun. 2023.

[15] MINAS GERAIS. Tribunal de Justiça. **Apelação Criminal nº 0131993-96.2017.8.13.0079**. Relatora: Desª. Maria Luiza de Marilac. Julgado em: 28 jan. 2025. Publicado em: 30 jan. 2025.

[16] BRASIL. Tribunal Regional Federal da 6ª Região (1. Seção Criminal). **Apelação nº 0000133-14.2019.4.01.3815**. Relator: Des. Fed. Rubens Rollo D'Oliveira. Julgado em: 22 abr. 2025. Publicado em: 22 abr. 2025.

> qualquer interlocutor que seja se passando por seu dono, a prova obtida dessa maneira arbitrária é ilícita (...)[17].

Conforme se observa em decisão proferida pelo Min. do STJ, Rogerio Schietti Cruz: “Sem mandado judicial, é ilícito o acesso tanto dos dados gravados acessados pela polícia ao manusear o aparelho, quanto dos dados eventualmente interceptados no momento em que ela acessa aplicativos de comunicação instantânea”[18].

O Des. Fed. José Lunardelli entende que, por mais que no “momento da prisão em flagrante, a autoridade policial tem o dever de apreender os objetos que tiverem relação com o fato, a teor do artigo 6º, II e III, do Código de Processo Penal”, para acessar os “dados e comunicações, contidos em memória de telefone celular” deve ser exigido autorização judicial. De acordo com a decisão proferida, cabe à autoridade policial, após realizar a apreensão dos aparelhos celulares, requerer “autorização judicial para afastar o sigilo do conteúdo do aparelho de telefonia móvel”[19].

Diante da necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação, o Ministro Gilmar Mendes, do STF, entendeu que a mera alegação pela autoridade de que o acesso aos dados armazenados em aparelho celular ocorreu com o consentimento do conduzido em estado de flagrante delito, de forma voluntária, não torna lícitas as provas obtidas. Assim, proferiu ordem para declarar a ilicitude das provas ilícitas e de todas dela derivadas[20]. Vale ressaltar que o STJ entende ser o ônus da acusação provar a autorização, não bastando, por si só, apenas o depoimento do policial alegando ter sido permitido o acesso, para que seja lícita a prova obtida[21].

Alinhado ao entendimento da Suprema Corte, o Des. Fed. André Custódio Nekatschalow ressaltou que apenas a afirmação da autoridade de que o aparelho teria sido entregue de forma voluntária pelo acusado, caso não esteja corroborada por outros meios de prova, não justifica a violação da intimidade[22].

Ademais, Aury Lopes Junior ensina que, nessas circunstâncias (flagrante e mandado), “o imputado jamais poderá ser compelido, nem mesmo por ordem judicial, a fornecer senhas, na medida em que protegido pelo direito de não autoincriminação” (Lopes Junior, 2025, p. 501).

3.2 Violação de aparelhos apreendidos em cumprimento de mandado de busca e apreensão

Quanto ao acesso aos dados armazenados em aparelhos celulares apreendidos mediante decisão judicial de busca e apreensão não exige nova autorização judicial específica para a quebra de sigilo desde que, na decisão que

---

[17] BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 511.484/RS**. Relator: Min. Sebastião Reis Júnior. Julgado em: 15 ago. 2019. Diário de Justiça Eletrônico, 29 ago. 2019.

[18] BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus nº 90.200/RN**. Relator: Min. Rogerio Schietti Cruz. Julgado em: 05 maio 2020.

[19] BRASIL. Tribunal Regional Federal da 3ª Região (4. Seção). **Embargos Infringentes e de Nulidade nº 0002421-63.2016.4.03.6181**. Relator: Des. Fed. José Lunardelli. Julgado em: 20 fev. 2020. Publicado em: 09 mar. 2020.

[20] BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus nº 168.052/SP**. Relator: Min. Gilmar Mendes. Julgado em: 20 out. 2020. Diário de Justiça Eletrônico, 02 dez. 2020.

[21] BRASIL. Superior Tribunal de Justiça (6. Turma). Habeas Corpus nº 674.185/MG. Relator: Min. Sebastião Reis Júnior. Julgado em: 17 ago. 2021.

[22] BRASIL. Tribunal Regional Federal da 3ª Região (5. Turma). **Apelação Criminal nº 5002827-98.2019.4.03.6114**. Relator: Des. Fed. André Custódio Nekatschalow. Julgado em: 10 maio 2022. Publicado em: 10 maio 2022.

autorizou a realização de busca e apreensão, esteja expressamente previsto a inclusão de documentos e mídias, bem como o afastamento do sigilo dos dados armazenados nos dispositivos apreendidos, tornando desnecessária nova autorização para sua análise.

Conforme salientou o Desembargador Federal André Luis Maia Tobias Granja, ao analisar a "decisão do Juízo da 36ª Vara Federal da Seção Judiciária de Pernambuco, que rejeitou a preliminar de nulidade das provas obtidas a partir do acesso a mensagens e dados armazenados em celulares apreendidos sem autorização judicial específica", entendeu que, "o acesso aos dados armazenados em aparelhos celulares apreendidos mediante decisão judicial de busca e apreensão não exige autorização judicial específica para a quebra de sigilo" desde que a busca e apreensão esteja acompanhada de decisão judicial expressa permitindo o acesso aos dados contidos nos dispositivos apreendidos.

De acordo com o Desembargador, a exigência de autorização judicial específica para quebra de sigilo aplica-se ao fluxo de comunicações, e não a dados estáticos armazenados em aparelhos regularmente apreendidos. Ou seja, a autoridade policial terá amplo acesso a todos os dados armazenados no aparelho, sem limitação temporal de acesso. Neste caso, deve ser analisada a decisão que determinou a busca e apreensão para que não ocorra uma verdadeira "*fishing expedition*", ou seja:

> [...] um indevido aproveitamento dos espaços de poder (investigatório estatal), para subversão da lógica do devido processo, pois serve para "vasculhar" a intimidade, a vida privada, o sigilo de dados, a proteção do domicilio etc., para além dos limites legais, em busca de qualquer elemento incriminatório, ainda que desconectado da causa inicial da investigação (Lopes Junior, 2025, p. 468).

Conforme analisado, em relação a aparelho apreendido no momento do flagrante ou em cumprimento de mandado de busca e apreensão, existem regras para o acesso e a extração dos dados. Adiante, veremos que, dos aparelhos em posse de um investigado, poderá, mediante ordem judicial, obrigar que o provedor responsável pela guarda dos dados disponibilize dados que possam contribuir para a identificação do usuário ou do terminal, entre outros relevantes ao processo, devendo quebrar o sigilo e encaminhar determinadas informações de um indivíduo (Brasil, 2014, art. 10, § 1°).

4 O FORNECIMENTO DE DADOS POR PROVEDORES PARA FINS DE PERSECUÇÃO PENAL

A quebra de sigilo telemático nada mais é do que a busca de dados que, reunidos, transformam-se em uma informação relacionada à determinado indivíduo. A Lei Geral de Proteção de Dados, no inciso I, do artigo 5º, diz que o dado pessoal é uma "informação relacionada à pessoa natural identificada ou identificável" (Brasil, 2018).

A doutrina, pela qual nos guiamos neste estudo, ensina que a "quebra do sigilo telemático sem fundamentação idônea e concreta" e a "interceptação telemática (e-mail) retroativa a período anterior àquele em que supostamente foram praticados os atos" investigados, dão "margem à varredura da intimidade e privacidade do investigado" e configuram uma verdadeira pesca probatória, conhecida mundialmente como "*fishing expedition*" (Lopes Júnior, 2025, p. 469).

Em obra clássica e pioneira de Alexandre Morais da Rosa, Viviani Ghizoni Silva e Philipe Benoni Melo e Silva, de acordo com Aury Lopes Júnior (2025), os autores definiram a "*fishing expedition*" como a "investigação especulativa indiscriminada, sem objetivo certo ou declarado, que 'lança' suas redes com a esperança de 'pescar' qualquer prova, para subsidiar uma futura acusação". Ou seja, é a antecipação de um procedimento investigativo ou repressivo que desrespeita a forma legal, atropela os requisitos previstos em nosso ordenamento jurídico, deteriora as garantias constitucionais, e distância a operacionalidade do Direito Penal das "balizas de um processo penal democrático de índole Constitucional" (Lopes Júnior, 2025, p. 468).

Devemos compreender que até mesmo as empresas estrangeiras que exploram serviços de internet em território brasileiro devem se submeter à Lei nº 12.965/2014 (Marco Civil da Internet) e torna-se desnecessário a cooperação internacional para a obtenção dos dados requisitados por um juízo. De acordo com o Des. Federal João Pedro Gebran Neto:

> por se submeterem à jurisdição brasileira, têm o dever de prestarem as informações determinadas por ordem de autoridade judiciária brasileira, que demanda a apresentação de dados necessários à apuração de crimes, quando o fato investigado foi praticado em território nacional e aqui é apurado[23].

O Marco Civil da Internet determinou que:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput**,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicia**l**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (Brasil, 2014)

De acordo com o § 3º, é possível o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. Ademais, importante se faz a observância do §2°, do art. 13:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo,

[23] BRASIL. Tribunal Regional Federal da 4ª Região (8. Turma). **Mandado de Segurança** nº 5019850-39.2019.4.04.0000. Relator: Des. Fed. João Pedro Gebran Neto. Julgado em: 03 out. 2019.

> em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput (Brasil, 2014).

No entanto, em nenhuma hipótese pode se confundir tais registros com dados telemáticos (conteúdo de *e-mail*, *imessages/hangouts*, fotos, contatos etc.). Conforme decidiu o Ministro Dias Toffoli sobre o congelamento de dados solicitado por representante do Ministério Público:

> [...] a ordem deve ser concedida para declarar a imprestabilidade dos elementos de prova obtidos a partir da requisição de preservação requisição de "congelamento" dos dados, de 26/02/2018 até 20/06/2022, foi encaminhado à empresa, sem prévia decisão judicial, revelando a nulidade apontada. Aliás a autorização judicial só foi proferida em 02/08/2022. Foi mencionado que a própria legislação pertinente ao caso determina que para que se tenha acesso ao conteúdo, para além de registros de conexão e acesso, o órgão ministerial necessitaria da prévia autorização judicial, conforme se extrai do artigo 10, § 1º, da referida Lei. (...) Por fim, considerando a ausência de autorização judicial prévia e levando-se em conta que a requisição, além de registros exclusivos, tais como informações de data e hora de acesso, duração e IP de origem, também solicitou a preservação de dados como fotos, vídeos, histórico de pesquisa, etc. protegidos pela privacidade e pela reserva de jurisdição, reconheceu-se que os limites legais foram extrapolados uma vez que tais informações não fazem parte do conceito de "registros de acesso a aplicações de internet" ou "registros de conexão". Assim, a ordem foi concedida para declarar a imprestabilidade dos elementos de prova obtidos a partir da requisição de preservação[24].

Perceba que o congelamento se mostra restrito apenas aos dados cadastrais que informem qualificação pessoal, filiação e endereço, se limitando apenas aos elementos permitidos pela lei, tais como registros de conexão e de acesso a aplicações de Internet. O Ministro do STF, Ricardo Lewandowski, no julgamento do HC 222.141, proferiu a seguinte decisão ao analisar a legalidade do requerimento feito pela GAECO[25]:

> Em hipótese alguma o "histórico de pesquisa, todo conteúdo de e-mail e iMessages, fotos, contatos e históricos de localização" podem ser considerados registros de acesso a aplicação de Internet. E mais, o próprio formato da requisição formulada pelo Ministério Público, buscando dados relativos a período que retroage mais de 5 anos, evidencia a desproporcionalidade do pedido e o descompasso entre a diligência efetuada e o permissivo legal[26].

Após compreendermos os limites do §3° do art. 10, da Lei 12.965/12, importante destacar que, caso a decisão judicial que determine a quebra do sigilo

---

[24] BRASIL. Supremo Tribunal Federal. **Reclamação nº 60.643/RJ**. Relator: Min. Dias Toffoli. Julgado em: 07 ago. 2023. Diário de Justiça Eletrônico, 09 ago. 2023.

[25] Sigla para Grupo de Atuação Especial de Combate ao Crime Organizado. Trata-se de um órgão investigativo vinculado ao Ministério Público (estadual ou federal), responsável por identificar, prevenir e reprimir as atividades de organizações criminosas, atuando em casos de maior complexidade e lesividade social.

[26] BRASIL. Supremo Tribunal Federal (2. Turma). **Agravo Regimental no Habeas Corpus nº 222.141/PR**. Relator: Min. Ricardo Lewandowski. Julgado em: 06 fev. 2024. Diário de Justiça Eletrônico, 03 abr. 2024.

telemático ou a interceptação telemática (*e-mail*) esteja carente de fundamentação, deverá ser determinado a "ilicitude das provas obtidas, na medida em que é um meio ilícito de obtenção de provas", devendo ser desentranhadas dos autos (Lopes Júnior, 2025, p. 469).

Torna-se relevante o conhecimento sobre a temática, pois a tese de ilicitude das provas deve ser arguida em tempo hábil, sob pena de se configurar nulidade de algibeira. Devemos compreender que a "alegação de nulidade processual", caso não seja pleiteada em tempo hábil, restará "prejudicada pela preclusão temporal, caracterizando 'nulidade de algibeira'". Isso porque, o princípio da boa-fé processual e da lealdade das partes impõe o dever de impugnar eventuais nulidades na primeira oportunidade, sob pena de preclusão, não sendo possível utilizá-las como argumento estratégico em momento posterior. Foi guiada por este princípio que a Desembargadora Federal Cibele Benevides Guedes da Fonseca decidiu que:

> A impetração do habeas corpus somente após o decurso de mais de dois anos da decisão que autorizou as medidas cautelares, mesmo após terem sido interpostos diversos outros incidentes e recursos pela mesma parte, caracteriza "nulidade de algibeira", prática processual vedada pela jurisprudência do STJ, por configurar estratégia defensiva tardia para questionar ato cuja legalidade poderia ter sido arguida oportunamente[27].

O Supremo Tribunal Federal, por meio da Ministra Rosa Weber, estabelece contornos para os limites temporais da busca de dados telemáticos. De acordo com a nobre Ministra, na decisão que determina a quebra de sigilo telemático, deve estipular um período proporcional, "com abrangência contemporânea às práticas delitivas denunciadas". Quanto à decisão, está pode ser "sucinta", mas deve se mostrar suficiente "quanto ao dever de fundamentação do artigo 93, IX, da Constituição Federal". Ademais, sustentou a posição do tribunal quanto a técnica 'per relationem'[28].

O Desembargador Federal José Lunardelli ensina que, a técnica '*per relationem*', se trata de uma fundamentação "mediante a qual se recorre ao corpo de decisões anteriores ou de manifestação ministerial como parcela substancial do próprio *decisum*"[29]

O Tribunal de Justiça do Distrito Federal entendeu que não é ilícita a quebra de sigilo telemático, no caso de investigação de crimes apenados com pena de reclusão e cometidos por organização criminosa, caso comprovado ser o único meio capaz de se prosseguir com as diligências[30].

Por sua vez, o Desembargador Jansen Fialho de Almeida, do Tribunal de Justiça do Distrito Federal, em análise de recurso promovido pelo Ministério Público após ter seu pedido de quebra de sigilo de dados de aparelho celular de um investigado por ato análogo a tráfico, pontuou que não basta uma mera alegação de

---

[27] BRASIL. Tribunal Regional Federal da 5ª Região (5. Turma). **Habeas Corpus nº 0800688-73.2025.4.05.0000**. Relatora: Des. Fed. Cibele Benevides Guedes da Fonseca. Julgado em: 11 fev. 2025.

[28] BRASIL. Supremo Tribunal Federal (1. Turma). **Agravo Regimental no Habeas Corpus nº 170.376/SP**. Relatora: Min. Rosa Weber. Julgado em: 08 jun. 2020. Diário de Justiça Eletrônico, 23 jun. 2020.

[29] BRASIL. Tribunal Regional Federal da 3ª Região (11. Turma). **Apelação Criminal nº 0003695-52.2009.4.03.6102**. Relator: Des. Fed. José Lunardelli. Julgado em: 18 jun. 2019. Publicado em: 04 jul. 2019.

[30] DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça (Câmara Criminal). **Habeas Corpus nº 0722055-34.2020.8.07.0000**. Relator: Des. Jair Soares. Julgado em: 07 out. 2020. Publicado em: 23 out. 2020.

que os investigados, “atual e usualmente, combinam encontros e transações lícitas e ilícitas por meio de seus aparelhos celulares”. Tal argumentação não possui elementos probatórios suficientes, “por si, para demonstrar a pertinência entre a quebra de sigilo de dados do aparelho telefônico requerida com a investigação”[31].

É salutar pontuar que os dados telemáticos, considerando seu potencial de exposição da intimidade e da vida privada, merece contornos sólidos, assim como o domicílio e as comunicações telefônicas e, de fato, uma mera decisão para tal violação não pode ser feita de forma sucinta.

Ora, devido sua relevância, é imprescindível que na decisão para quebra de sigilo telemático, assim como têm entendido os tribunais no tocante às interceptações telefônicas (Brasil, 1996), demonstre sua conveniência e indispensabilidade e apresente claramente os motivos e limites, devendo atender os “requisitos para a sua concessão, quais sejam, indícios razoáveis de autoria ou participação em infração penal, imprescindibilidade da medida e o fato investigado deve constituir crime punido com reclusão, nos termos do art. 2º da Lei nº 9.296/96”[32]. Sobre o tema, o STF tem entendido da seguinte forma:

> AGRAVO INTERNO EM HABEAS CORPUS. INTERCEPTAÇÃO TELEFÔNICA. FUNDAMENTAÇÃO IDÔNEA. HABEAS CORPUS INDEFERIDO. 1. A interceptação telefônica, prevista no art. 5º, XII, da Constituição da República e regulamentada pela Lei n. 9.296/1996 (Lei de Interceptação Telefônica), quando autorizada, “deverá ser expedida pelo juiz competente, em decisão devidamente fundamentada que demonstre sua conveniência e indispensabilidade” (HC 130.596 AgR, ministro Alexandre de Moraes), sob pena de nulidade do ato jurisdicional. 2. A violabilidade das comunicações telefônicas só poderá ocorrer excepcionalmente, desde que (i) estejam presentes indícios razoáveis da autoria ou da participação do investigado em infração penal; (ii) inexista outro meio para obtenção de prova; e (iii) configure o fato em apuração crime punido com reclusão**.** 3. É inadmissível, na via estreita do habeas corpus, a qual não comporta dilação probatória, o reexame, com vistas ao acolhimento da tese defensiva – quebra do sigilo telefônico com base apenas em denúncia anônima –, do conjunto fático-probatório produzido na origem, notadamente porque ressaltada pelas instâncias ordinárias a existência de provas e investigações prévias, e especificados os motivos que, à época, evidenciavam a necessidade da quebra do sigilo das ligações telefônicas. 4. Agravo interno desprovido[33].

De acordo com o Desembargador Marcus Vinicius de Lacerda Costa:

> O procedimento de que trata o art. 2º da Lei n. 9.296/1996, cujas rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplicam a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet[34].

---

[31] DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça (3. Turma Criminal). **Habeas Corpus nº 0708122-86.2023.8.07.0000**. Relator: Des. Jansen Fialho de Almeida. Julgado em: 25 maio 2023. Publicado em: 05 jun. 2023.

[32] MINAS GERAIS. Tribunal de Justiça. **Habeas Corpus nº 5001417-85.2024.8.13.0239**. Relatora: Desª. Amalin Aziz Sant'Ana. Julgado em: 30 jan. 2025. Publicado em: 06 fev. 2025.

[33] BRASIL. Supremo Tribunal Federal (2. Turma). **Agravo Regimental no Habeas Corpus nº 212.702/DF**. Relator: Min. Nunes Marques. Julgado em: 16 maio 2022. Diário de Justiça Eletrônico, 02 jun. 2022.

[34] PARANÁ. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus nº 0035059-28.2023.8.16.0000**. Relator: Des. Marcus Vinicius de Lacerda Costa. Julgado em: 24 ago. 2023. Publicado em: 24 ago. 2023.

Ademais, ressalta que:

> Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios[35].

Ora, na decisão analisada, foi considerado que “a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas”, pois, de fato, o “objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado”[36].

Importante ressaltar que os mecanismos tecnológicos e a deficiência de regras para utilização de aplicativos, ao não regular o processo de identificação de identidade dos usuários, corrobora com o “processo migratório”[37] da criminalidade para o mundo digital. A utilização de tais recursos mitiga a capacidade de individualizar a conduta delituosa e identificar o indivíduo, sendo este o motivo pelo qual ocorre deferimento da medida cautelar (a busca pela real identidade do autor).

Entretanto, há hipóteses em que o requerimento deveria indicar a identidade do investigado no momento em que se solicita a quebra de sigilo, sob pena de se violar direito de terceiros. Tal medida torna-se viável tendo em vista que possibilita a mitigação de arbitrariedades. Ora, nos procedimentos investigatórios em que o autor se mostra identificado, deve ser identificado para evitar a violação da intimidade de terceiros pela empresa provedora de serviços digitais.

Assim, torna-se relevante para o Estado Democrático de Direito que a ordem judicial especifique previamente a(s) pessoa(s) e objetos que são pertinentes à investigação e, que, a prova da infração (ou da autoria) não possa ser realizada por outros meios. Tais requisitos devem ser demonstrados por meio de decisão fundamentada, que demonstre a necessidade de se proceder o feito.

Ora, nota-se que não há diretrizes legais suficientes para tutelar um direito de tamanha relevância, que possibilita ir além do que se encontra em um domicílio e do que se extrai das comunicações.

---

[35] PARANÁ. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus nº 0035059-28.2023.8.16.0000**. Relator: Des. Marcus Vinicius de Lacerda Costa. Julgado em: 24 ago. 2023. Publicado em: 24 ago. 2023.

[36] PARANÁ. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus nº 0035059-28.2023.8.16.0000**. Relator: Des. Marcus Vinicius de Lacerda Costa. Julgado em: 24 ago. 2023. Publicado em: 24 ago. 2023.

[37] Investigadores da PF e da Interpol (rede internacional de polícias) dizem à CNN que essa migração está relacionada à facilidade de se cometer um crime de lavagem de dinheiro, por exemplo, ocultação de bens ou realizar pagamentos no exterior. (Maia, 2025).

Outrossim, devemos pontuar que uma denúncia anônima não possui robustez para justificar a quebra de sigilo telemático. Assim, deve haver diligências posteriores à denúncia que comprovem os fatos informados bem como a necessidade de se proceder o feito e a proporcionalidade em que o feito será realizado. Conforme ensina o renomado doutrinador Guilherme de Souza Nucci: “Havendo a denúncia anônima, cabe aos agentes policiais a investigação de sua veracidade, para, então, instaurar regularmente o inquérito policial e colher provas” (Nucci, 2025, p. 23). Ou seja, nem mesmo a abertura de um inquérito pode se dar por meio de uma denúncia anônima.

É pertinente ao debate a utilização dos meios de produção de provas não inseridos na legislação. Torna-se incoerente com o ordenamento a decisão que determina o afastamento do sigilo telemático de conversas privadas (Brasil, 2014, art. 7º, III), ativando, de forma compulsória, mecanismos (armazenamento em nuvem) que só poderiam ser acionados pelo detentor do aparelho, uma vez que este pode escolher entre compartilhar ou não seus dados com o provedor de serviço. Essa decisão que autoriza a produção compulsória ainda pode determinar que a empresa impeça o usuário de realizar sua desativação.

Acionar funções como a sincronização automática da conta *iCloud* e/ou em nuvem é uma clara violação ao princípio *nemo tenetur se detegere.* Este que determina que ninguém é obrigado a produzir provas contra si mesmo. O Ministro Reynaldo Soares da Fonseca ensina que se trata de um “princípio de caráter processual penal, já que intimamente ligado à produção de provas incriminadoras”. Trata-se de:

> [...] uma garantia da não autoincriminação, segundo o qual ninguém é obrigado a produzir prova contra si mesmo, ou seja, ninguém pode ser forçado, por qualquer autoridade ou particular, a fornecer involuntariamente qualquer tipo de informação ou declaração que o incrimine, direta ou indiretamente[38].

Ademais, diferentemente dos dados estáticos extraídos de aparelhos apreendidos, não há previsão legal que permita o Estado ir além da coleta dos dados criados e já autorizados a ativação pelo usuário do compartilhamento e armazenamento pela empresa provedora de serviços na rede.

O art. 7º, da Lei 12.965/2014, que regulamenta o afastamento do sigilo telemático de conversas privadas, diz que “O acesso à internet é essencial ao exercício da cidadania” e em seu inciso III estabelece o direito à “inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial”. Portanto, não há previsão para que o Estado obrigue o investigado a produzir provas contra si mesmo.

Em decisão proferida pelo juiz Paulo Roberto Caixeta, da 4º Vara Criminal da Comarca de Uberlândia MG, nos autos do processo nº 702.20.009668-4, determinou a quebra de sigilo da seguinte forma:

> Preservação e envio de todo o conteúdo armazenado em “nuvem” iCLOUD, bem como ativar/habilitar a SINCRONIZAÇÃO AUTOMÁTICA da (s) conta (s) indicada (s) ou vinculada (s) ao (s) IMEI (s) informado (s), de forma compulsória e velada ao usuário[39].

---

[38] BRASIL. Superior Tribunal de Justiça (5. Turma). **Embargos de Declaração no Habeas Corpus nº 808.612/SP**. Relator: Min. Reynaldo Soares da Fonseca. Julgado em: 08 ago. 2023.

[39] Disponível em: https://drive.google.com/file/d/18HWa9JCejAfMuKfGlFpTerZX5IyuO5ay/view?usp=sharing

Uma das maiores empresas provedoras de dados, a *Google*, afirma que não é possível “efetuar um *backup* forçado”. Ademais, esclarece “que não possui capacidade técnica para fazer com que um dispositivo seja objeto de tal interferência contra a vontade do usuário” (Sampaio; Santos Júnior, 2024).

Devemos compreender que o Marco Civil da Internet não autoriza procedimentos que visam além da “coleta” em específico, ou seja, não concede poderes para que o juiz, por meio de sua decisão, possa determinar que a empresa ative mecanismos para fazer com que o investigado, sem seu consentimento, armazene provas, de forma coercitiva e, o suspeito, de forma involuntária. Conforme leciona Aury Lopes Junior (2025):

> [...] no processo penal existe exercício condicionado e limitado de poder, sob pena de autoritarismo. E esse limite vem dado pela “forma”. Portanto, flexibilizar a forma é abrir a porta para que os agentes estatais exerçam o poder sem limite, em franco detrimento dos espaços de liberdade. É rasgar o princípio da legalidade e toda a teoria da tipicidade dos atos processuais. É rasgar a Constituição (Lopes Junior, 2025, p. 46).

Em síntese, proceder a criação de um backup compulsório, além de violar o princípio da não autoincriminação, ignora o princípio da legalidade, que é a base do nosso Estado Democrático de Direito.

5 CONSIDERAÇÕES FINAIS

A presente análise percorreu decisões proferidas pelas cortes superiores e por vários tribunais estaduais (STF, STJ, TJSC, TJMG, TRF3, TRF4, TRF5, TRF6, TJDFT, TJPR), relacionadas ao tema e, dentre elas, foram selecionadas e utilizadas aquelas que, pelo rigor técnico utilizado, se mostraram necessárias para o estudo.

Observamos que a expansão de práticas investigativas que utilizam da intimidade construída no mundo digital para obtenção de provas pode ocorrer em circunstâncias e cenários distintos. O atual cenário jurisprudencial exala insegurança jurídica pois, de fato, a proteção da intimidade digital não alcançou contornos legais sólidos e coerentes com a ordem jurídica constitucional.

Gilmar Mendes, Decano do Supremo Tribunal Federal, em sustentação oral na reclamação 73.295, destacou que o excesso de reclamações, em alguns casos, se dá por uma disputa infantil de certos tribunais ou turmas com o STF, por razões sem sentido. Logo, por mais que haja diversas decisões pontuando a necessidade de autorização judicial, ainda há decisões em sentido contrário.

Não se pode admitir a flexibilização dos limites da atuação policial e legitimar que, ao apreender alguém em flagrante delito, o agente do Estado atenda uma ligação telefônica (que atualmente se faz por aplicativos conectados à internet). Não há nenhuma previsão legal que legitime tal ação arbitrária.

Inadmissível, de igual forma, que se passe pela pessoa abordada e realize negociações de compra ou venda de drogas para provocar o flagrante em terceiros, porquanto ilícito. Assim, por mais que não configure interceptação telefônica, conforme salienta o Desembargador Rubens Rollo D’Oliveira, temos que além de se exigir autorização judicial prévia, é necessária uma permissão legal para o feito, o que até o momento inexiste em nosso ordenamento.

O cumprimento de mandado de busca e apreensão não pode ser confundido com o mandado de prisão. Para acessar o dispositivo do indivíduo que já tem prisão

decretada deverá ser observado a necessidade de autorização judicial específica, o que não ocorre no caso dos aparelhos que são apreendidos no mandado de busca e apreensão. Em ambos os casos, deve-se atentar para que a medida não se configure mera *fishing expedition.*

Ademais, esclarecemos que os registros de conexão previstos no §2°, do art. 13, do Marco Civil da Internet, em nenhuma hipótese, podem confundir tais registros com dados telemáticos (conteúdo de *e-mail, imessages/hangouts*, fotos, contatos etc.). A problemática central, no tocante à intimidade digital, ocorre quanto aos deveres das empresas que controlam aplicativos que podem ter acesso a dados pessoais.

Como vimos, o armazenamento compulsório não possui respaldo legal, porém decisões podem determinar que as empresas realizem o feito e façam com que o investigado produza provas contra si mesmo, pois mesmo que não tenha permitido o acesso da empresa a tais dados, ela será cogitada a armazená-los.

Pontuamos que a decisão que determina a quebra de dados telemáticos deve respeitar: i) a proporcionalidade - os dados devem ter abrangência contemporânea às práticas delitivas denunciadas; e ii) a necessidade - deve-se demonstrar que o feito é necessário para elucidar o contexto criminoso.

Ocorre que o Marco Civil da Internet não determina que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios. Para a jurisprudência, a decisão deve indicar os seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros.

Devido ao vasto conteúdo que pode ser acessado com a relativização da intimidade, para que o feito se realize em conformidade com a Constituição, deveria determinar que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação (salvo impossibilidade, que deverá ser demonstrada), e que justifique a indispensabilidade da medida, ou seja, deveria demonstrar que a prova da infração não pode ser realizada por outros meios.

Assim, por mais que tenham ocorrido grandes avanços quanto à proteção da intimidade, essa proteção ainda não alcançou os parâmetros constitucionais que regem nosso ordenamento.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília-DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 nov. 2025.

BRASIL. **Decreto nº 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 16 dez. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 22 nov. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 22 nov. 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília-DF, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 22 nov. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília-DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 nov. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília-DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 03 dez. 2025.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo em Recurso Especial nº 2.697.584/MG**. Penal e processual penal. Agravo em recurso especial. Tráfico de entorpecentes. Nulidade. Provas obtidas através de acesso a dados constantes no aparelho celular, sem autorização judicial. Violação à lei federal configurada. Agravo conhecido para dar provimento ao recurso especial. Relatora: Min. Daniela Teixeira. Julgado em: 17 dez. 2024. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=2697584&O=JT. Acesso em: jan. 2025.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Embargos de Declaração no Habeas Corpus nº 808.612/SP**. Embargos de declaração no habeas corpus. Omissão. Advertência quanto ao direito de não autoincriminação. Vício constatado. Nulidade relativa. Prejuízo não demonstrado. Embargos acolhidos. Sem efeitos modificativos. Relator: Min. Reynaldo Soares da Fonseca. Julgado em: 08 ago. 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202300816787&dt_publicacao=14/08/2023. Acesso em: 16 dez. 2025.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 511.484/RS**. Habeas corpus. Tráfico de drogas. Sentença transitada em julgado. Ilicitude da prova. Ausência de autorização pessoal ou judicial para acessar dados do aparelho telefônico apreendido ou para atender ligação. Policial passou-se pelo dono da linha e fez negociação para provocar prisão em flagrante. Inexistência de prova autônoma e independente suficiente para a condenação. Relator: Min. Sebastião Reis Júnior. Julgado em: 15 ago. 2019. Diário de Justiça Eletrônico, 29 ago. 2019. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201901452520&dt_publicacao=29/08/2019. Acesso em: 16 dez. 2025.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 617.232/SP**. Relator: Min. Nefi Cordeiro. Julgado em: 23 fev. 2021. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?

tipo_documento=documento&componente=MON&sequencial=116126070&num_registro=202002602998&data=20201006. Acesso em: 16 dez. 2025.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 674.185/MG**. Relator: Min. Sebastião Reis Júnior. Julgado em: 17 ago. 2021. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=129132174&num_registro=202101864837&data=20210621. Acesso em: 16 dez. 2025.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus nº 90.200/RN**. Recurso em habeas corpus. Tráfico de drogas. Presos em flagrante que tiveram seus telefones celulares acessados pela polícia sem mandado judicial. Nulidade. Ocorrência. Recurso provido. Relator: Min. Rogerio Schietti Cruz. Julgado em: 05 maio 2020. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1904522&num_registro=201702542071&data=20200512&formato=PDF. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal (1. Turma). **Agravo Regimental no Habeas Corpus nº 170.376/SP**. Agravo regimental no habeas corpus. Quebra de sigilo telemático. Fundamentação. Técnica per rationem. Período de quebra. Proporcionalidade. Máteria fática estabilizada. Negativa de seguimento ao habeas corpus. Julgamento monocrático. Possibilidade. Relatora: Min. Rosa Weber. Julgado em: 08 jun. 2020. Diário de Justiça Eletrônico, 23 jun. 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753054975. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). **Agravo Regimental no Habeas Corpus nº 212.702/DF**. Relator: Min. Nunes Marques. Julgado em: 16 maio 2022. Diário de Justiça Eletrônico, 02 jun. 2022. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=761091463. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). **Agravo Regimental no Habeas Corpus nº 222.141/PR**. Relator: Min. Ricardo Lewandowski. Julgado em: 06 fev. 2024. Diário de Justiça Eletrônico, 03 abr. 2024. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=775652964. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus nº 168.052/SP**. Relator: Min. Gilmar Mendes. Julgado em: 20 out. 2020. Diário de Justiça Eletrônico, 02 dez. 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754545381. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus nº 74.639-0/RJ**. Relator: Min. Marco Aurélio. Julgado em: 31 out. 1996. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=75387. Acesso em: 16 dez. 2025.

BRASIL. Supremo Tribunal Federal. **Reclamação nº 60.643/RJ**. Relator: Min. Dias Toffoli. Julgado em: 07 ago. 2023. Diário de Justiça Eletrônico, 09 ago. 2023. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho1432728/false. Acesso em: 16 dez. 2025.

BRASIL. Tribunal Regional Federal da 3ª Região (11. Turma). **Apelação Criminal nº 0003695-52.2009.4.03.6102**. Relator: Des. Fed. José Lunardelli. Julgado em: 18 jun. 2019. Publicado em: 04 jul. 2019.

BRASIL. Tribunal Regional Federal da 3ª Região (4. Seção). **Embargos Infringentes e de Nulidade nº 0002421-63.2016.4.03.6181**. Relator: Des. Fed. José Lunardelli. Julgado em: 20 fev. 2020. Publicado em: 09 mar. 2020.

BRASIL. Tribunal Regional Federal da 3ª Região (5. Turma). **Apelação Criminal nº 0003512-51.2013.4.03.6002**. Relator: Des. Fed. Paulo Gustavo Guedes Fontes. Julgado em: 18 set. 2020. Publicado em: 24 set. 2020.

BRASIL. Tribunal Regional Federal da 3ª Região (5. Turma). **Apelação Criminal nº 5002827-98.2019.4.03.6114**. Relator: Des. Fed. André Custódio Nekatschalow. Julgado em: 10 maio 2022. Publicado em: 10 maio 2022.

BRASIL. Tribunal Regional Federal da 4ª Região (7. Turma). **Habeas Corpus nº 5018214-96.2023.4.04.0000/RS**. Relator: Des. Fed. Angelo Roberto Ilha da Silva. Julgado em: 22 jun. 2023. Disponível em: https://eproc.trf4.jus.br/eproc2trf4/controlador.php?acao=acessar_documento_publico&doc=416875320970606214105766000 35&evento=40400188&key=29d27a607dc567817ce450622d8db20558e82f7e311f1bb053a8f733133a764e&hash=70a0d96b4146b8bdddb0027b42657c84. Acesso em: 16 dez. 2025.

BRASIL. Tribunal Regional Federal da 4ª Região (8. Turma). **Mandado de Segurança nº 5019850-39.2019.4.04.0000**. Relator: Des. Fed. João Pedro Gebran Neto. Julgado em: 03 out. 2019.

BRASIL. Tribunal Regional Federal da 4ª Região (8. Turma). **Mandado de Segurança nº 5045005-39.2022.4.04.0000**. Relator: Des. Fed. Carlos Eduardo Thompson Flores Lenz. Julgado em: 01 mar. 2023. Publicado em: 02 mar. 2023. Disponível em: https://eproc.trf4.jus.br/eproc2trf4/controlador.php?acao=acessar_documento_publico&doc=416777683403302871568160683 16&evento=40400188&key=538a95456c2865967b96c7e5d49f9c58f25d77ec4752f80878f150bf3af7f9b5&hash=9faf645e8fa7e673e8710d748de783ca. Acesso em: 16 dez. 2025.

BRASIL. Tribunal Regional Federal da 5ª Região (5. Turma). **Habeas Corpus nº 0800688-73.2025.4.05.0000**. Relatora: Des. Fed. Cibele Benevides Guedes da Fonseca. Julgado em: 11 fev. 2025. Disponível em: https://pje.trf5.jus.br/pjeconsulta/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?signedIdProcessoTrf=6812ada90dee3c387693329b2ebbdbc5. Acesso em: 16 dez. 2025.

BRASIL. Tribunal Regional Federal da 6ª Região (1. Seção Criminal). **Apelação nº 0000133-14.2019.4.01.3815**. Relator: Des. Fed. Rubens Rollo D'Oliveira. Julgado em: 22 abr. 2025. Publicado em: 22 abr. 2025.

DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça (3. Turma Criminal). **Habeas Corpus nº 0708122-86.2023.8.07.0000**. Relator: Des. Jansen Fialho de Almeida. Julgado em: 25 maio 2023. Publicado em: 05 jun. 2023.

DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça (Câmara Criminal). **Habeas Corpus nº 0722055-34.2020.8.07.0000**. Relator: Des. Jair Soares. Julgado em: 07 out. 2020. Publicado em: 23 out. 2020.

LOPES JUNIOR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025. E-book. p.511. ISBN 9788553625673. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/. Acesso em: 20 nov. 2025.

LOPES JUNIOR., Aury. **Fundamentos Do Processo Penal** - Introdução Crítica. 11. ed. Rio de Janeiro: SRV, 2025. E-book. p.46. ISBN 9788553625611. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625611/. Acesso em: 30 nov. 2025.

MAIA, Elijonas. PF mapeia migração de organizações criminosas para crimes cibernéticos. **CNN Brasil**, 14 mar. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil/pf-mapeia-migracao-de-organizacoes-criminosas-para-crimes-ciberneticos/#goog_rewarded. Acesso em: 16 dez. 2025.

MINAS GERAIS. Tribunal de Justiça (4. Vara Criminal da Comarca de Uberlândia). **Processo nº 702.20.009668-4**. Juiz Paulo Roberto Caixeta. [s.d.].

MINAS GERAIS. Tribunal de Justiça. **Apelação Criminal nº 0131993-96.2017.8.13.0079**. Relatora: Desª. Maria Luiza de Marilac. Julgado em: 28 jan. 2025. Publicado em: 30 jan. 2025.

MINAS GERAIS. Tribunal de Justiça. **Habeas Corpus nº 5001417-85.2024.8.13.0239**. Relatora: Desª. Amalin Aziz Sant'Ana. Julgado em: 30 jan. 2025. Publicado em: 06 fev. 2025.

MORAES, Alexandre de. **Direito Constitucional**. 41. ed. Rio de Janeiro: Atlas, 2025. E-book. p.74. ISBN 9786559777143. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559777143/. Acesso em: 26 out. 2025.

MORAIS, Felipe. Sigilo de dados: os limites do poder de requisição do delegado de polícia e membro o Ministério Público. **Jus.com.br**, 2022. Disponível em: https://jus.com.br/artigos/99790/sigilo-de-dados-os-limites-do-poder-de-requisicao-do-delegado-de-policia-e-membro-do-ministerio-publico. Acesso em 20. nov. 2025.

NUCCI, Guilherme de S. **Código de Processo Penal Comentado.** 24. ed. Rio de Janeiro: Forense, 2025. E-book. p.359. ISBN 9788530996444. Disponível em:

https://integrada.minhabiblioteca.com.br/reader/books/9788530996444/. Acesso em: 21 nov. 2025.

ONU. Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos.** Paris: ONU, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos. Acesso em: 16 dez. 2025.

PARANÁ. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus nº 0035059-28.2023.8.16.0000**. Relator: Des. Marcus Vinicius de Lacerda Costa. Julgado em: 24 ago. 2023. Publicado em: 24 ago. 2023.

SAMPAIO, Denis; SANTOS JR., Antônio. Backup forçado e velado de dados em investigações: um tema delicado. **Consultor Jurídico**, 2024. Disponível em: https://www.conjur.com.br/2024-jun-22/backup-forcado-e-velado-de-dados-em-investigacoes-um-tema-delicado/. Acesso em: nov. 2025.

SANTA CATARINA. Tribunal de Justiça (5. Câmara Criminal). **Habeas Corpus Criminal nº 5033494-87.2021.8.24.0000**. Relator: Des. Antônio Zoldan da Veiga. Julgado em: 15 jul. 2021.